REMARKS

Applicants thank the Examiner for the Office Action of November 18, 2008. This Amendment is in full response thereto. Thus, Applicants respectfully request continued examination and allowance of the application.

Claims 28-32 are pending in this application. The claims have been amended to correct some antecedent basis issues. No new matter has been added by these amendments.

First Claim Rejection Under 35 U.S.C. § 103:

Claims 28-29 and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Birkle, et al (US Pub. No. 2003/0023333) (Birkle) in view of Sultan (USPN 7,058,973). Applicants respectfully disagree because the combination of Birkle and Sultan fails to teach all of the claim limitations of claims 28, 29 and 31 and furthermore because both Birkle and Sultan teach away from the Examiner's suggested combination.

Claim 28

With respect to claim 28, the Examiner alleges that Birkle teaches:

assigning a unique network address to said router for devices outside the EAN (step D) at page 2, para 25; Fig. 3, tag 10; control server also has a web server that has an IP address;

connecting a local HMI Web browser to said router (step E) at page 2, para 22-23; page 3, para 32; and

configuring said router to receive requests from Web browsers both local and remote to said EAN (step F) at page 2, para 22-23.

Applicants respectfully disagree. Steps D, E and F refer to the router of step C (connecting a local router between said Web server and a computer network), which

the Examiner alleges is taught by Sultan at col. 7, lines 44-63. However, as the Examiner relies on Sultan to provide the router of Step C, Birkle alone cannot provide the teachings of steps D, E, and F because Birkle does not assign a unique network address to a **router** (step D), does not connect a local HMI Web browser to the **router** (step E), and does not configure the **router** to receive requests from Web browsers both local and remote to the EAN (step F).

In fact, as the Examiner points out with respect to step D, Birkle assigns a unique network address to the web server of its control server, not to a router. Additionally, as quoted below, tag 10 of Figure 3 refers to a control unit, not a router. At page 2, para 0025, Birkle states:

> **The WEB servers (13) have a separate IP address each and can be accessed directly**. Bridges and rooters, with which the entire data network (16) can be segmented into smaller deterministic data networks, may be integrated in the data network (16). Moreover, the rooters control the data traffic while setting priorities and give priority to the time-critical control data before other data. As a result, a very rapid and purposeful exchange of the control data can be achieved. The control data being exchanged during the control operations consist of, e.g., control commands of the **control units** (**10**, 14, 25) and feedback of the accessed receivers. These may be, e.g., acknowledgments of receipt, and a so-called handshake may also be performed to check and secure the data traffic. In addition, the receivers report the performance of the control commands back to the **control units** (**10**, 14, 25), which is likewise monitored with a handshake. Furthermore, diagnosis data, programs or other data may be exchanged as well.

As a result, the Examiner's alleged support does not provide the limitations of Applicants' step D. Furthermore, per the citation and for future reference, Birkle utilizes the bridges and rooters to segment the data network 16 into smaller deterministic data networks to better control data traffic resulting in a rapid and purposeful exchange. This teaching does not lead one of ordinary skill in the art to conclude that Birkle connects a router between a Web server and a computer network.

The Examiner cites page 2, paras 0022 and 0023 and page 3, para 0032 as allegedly disclosing the limitations of steps E and F. However, Birkle makes no mention of a rooter at page 2, paras 0022 to 0023:

> The WEB control system (2) comprises a plurality of WEB servers (13) associated with the intelligent application components (3) with at least one homepage (17) each belonging to them and with at least one interface (15) each for the connection to the data network (16). Each intelligent system component (3) preferably has a WEB server (13) of its own here with at least one homepage (17) of its own. Suitable display and operating devices (22) may be associated with the WEB servers (13). As an alternative or in addition, one or more separate display and operating devices (22) may be present and connected to the data network (16).
>
> The display and operating devices (22) and the WEB servers (13) are equipped with a suitable communications software. In particular, WEB browsers for displaying and operating the corresponding homepages (17) are installed on the display and operating devices (22). The data network (16) is preferably designed as a Fast Ethernet data network using the TCP/IP protocol. The interfaces (15) are also designed correspondingly and are designed, e.g., as Fast Ethernet plug cards. The above-mentioned components correspond to the common Internet standards in terms of software and hardware. In case of a change in the Internet standards, a corresponding adaptation of the components may be performed.

Additionally, Birkle makes no mention of a rooter at page 3, para 0032:

> The control parts (25) of the intelligent application components (3) have at least one computer (14) each, which is preferably designed as a personal computer, especially an industrial PC, or, in a simpler design, as a microprocessor. The computers (14) may have suitable, directly connected input and output devices (22), so-called HMI (human-machine interfaces). These are, e.g., a keyboard, a mouse, a marker pen, and suitable display devices, which are preferably designed as screens with graphics capability, e.g., as touch screens.

As a result, the Examiner's alleged support does not teach the limitations of Applicants' steps E and F.

As step C of Applicants' claim 28 expressly requires a router between the computer network and the local WEB server, as Birkle expressly teaches assigning

IP addresses to its Web servers for communication purposes, and as Birkle only utilizes a router to segment a data network, Birkle does not anticipate or render obvious the limitations required in steps D, E, and F of independent claim 28 that expressly utilize a router.

The Examiner alleges that Birkle only fails to teach Network Address Translation (step I). Applicants respectfully disagree. Per the discussion above, Birkle fails to disclose the limitations of step C, connecting a local router between said Web server and a computer network, and, as a result, further fails to disclose the limitations of steps D, E, and F.

The Examiner alleges that Sultan teaches connecting a local router between said web server and a computer network at col. 7, lines 44-63. Applicants respectfully disagree. Sultan teaches connecting a local area network to a computing site on the internet through a gateway. Nowhere in lines 44-63 does Sultan mention a web server.

> In FIG. 1, a virtual private network (VPN) is shown in which a private local area network (LAN) 10 is connected to a computing site 30 located on the internet 50. The LAN 10 uses local IP addresses, and is connected to the internet through the network address translation (NAT) gateway of this invention 20. The computing site 30 may be a business headquarters, or one of any number of private LANs used by a multinational corporation, an educational facility, or any other site which will be frequently accessed from remote locations. Such sites will normally have a firewall or gateway 35 capable of running encryption and other security applications. Such a gateway will have the ability to open a packet, decrypt or otherwise access its contents, and perform address translation, routing, de-encapsulation, and data manipulation functions as well. While such devices are able to support ISAKMP and other IPSec protocols, they do so by opening and decrypting packets, and manipulating data, and are, by and large, too expensive and powerful to be employed efficiently at remote LAN sites needing to establish a VPN with the main computing site.

As a result, the Examiner's alleged support does not provide the limitations of Applicants' step C. Additionally, nothing in Sultan would lead one of ordinary skill in

the art to connect the gateway/router to each Web server/controller/equipment, as is required by claim 28.

The Examiner alleges that it would have been obvious to one of ordinary skill in the art at the time of the invention to create the method of Birkle to include network address translation as taught by Sultan in order to pass information across the internet in a secure manner. While this may be true, as discussed above, the combination of Birkle and Sultan does not render obvious the limitations of Applicants' claim 28.

Additionally, the combination of Birkle and Sultan teaches away from Applicants' claim limitations. In particular, Sultan states at col. 2, lines 28-33 that, due to explosive use of the internet, unique IP addresses are becoming scarce. Sultan further teaches employing a single globally unique address to be used on the internet by the gateway separating the LAN from the internet (col .2, lines 38-41). As stated previously, Birkle utilizes the bridges and rooters to segment the data network 16 into smaller deterministic data networks to better control data traffic resulting in a rapid and purposeful exchange. Based on the combined teachings of Birkle and Sultan, one of ordinary skill in the art may utilize the network address translation taught by Sultan in the method of Birkle. However, such combination would not render obvious Applicants' method that requires, *for each local piece of equipment*, (A) connecting a local controller to the piece of equipment, (B) connecting a local Web server to the controller, (C) *connecting a local router* between the Web server and a computer network, (D) *assigning a unique network address to said router for devices outside the EAN*, (E) *connecting a local HMI Web browser to said router*, (F) *configuring said router to receive requests from Web browsers both local and remote to said EAN*, (G) responding to a request from a Web browser *by having said router* check the source network address of the requesting Web browser, (H) determining in response to a requesting local Web browser a destination network address it is

requesting, (I) *configuring said router* to respond to the destination network address of a remote Web server by using network address translation (NAT) to translate the source network address of the requesting local Web browser, (J) forwarding the request *via said router* to said remote Web server, (K) receiving *via said router* a response from said remote Web server that it received the request, and (L) forwarding the response to the local Web browser of said EAN.

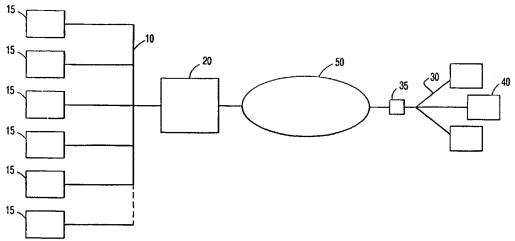
If anything, the combination of Birkle and Sultan would lead one of ordinary skill in the art to utilize fewer gateways/routers, not one for each local piece of equipment, or to utilize Sultan's NAT on Birkle's directly accessible Web servers, not on Birkle's routers.

The Examiner alleges in the remarks section of the Office Action that the Birkle reference implies providing isolation and allowing selective communication on page 2, para 25. As discussed previously with respect to that paragraph, Birkle expressly teaches that routers may be added to a network to speed up communications on that network. Applicants respectfully request additional information as to how that teaching implies isolation. Nothing in that paragraph would lead one of ordinary skill in the art to utilize a router to isolate a piece of equipment and its associated controller and web server. Additionally, as Birkle's servers each have unique IP addresses, it is not clear whether Birkle's routers are utilized to communicate with an outside network or merely exchanges control data internally. ("Moreover, the rooters control the data traffic while setting priorities and give priority to the time-critical control data before other data. ... The control data being exchanged during the control operations consist of, e.g., control commands of the control units (10, 14, 25) and feedback of the accessed receivers."). As a result, even if Birkle utilizes his rooters to provide isolation as the Examiner alleges, it is not clear that Birkle would assign a unique network address to a **router** (step D), connect a local HMI Web browser to the **router** (step E), and configure the **router** to receive

requests from Web browsers both local and remote to the EAN (step F), especially since Birkle expressly teaches that his "...**WEB servers (13) have a separate IP address each and can be accessed directly.**"

In his remarks, the Examiner alleges that Sultan explicitly details the idea of a router between a network and a **website** at col. 7, lines 44-63. Applicants agree. Applicants have claimed connecting a router between a **Web server** and a computer network, and more specifically to the claimed Web server that is connected to the controller and the piece of equipment. Therefore, Sultan's teachings neither anticipate nor render obvious Applicants' claim.

Finally, the Examiner states "the term local does not specifically denote where it is located. While Sultan can be interpreted according to Figure 1, the router, tag 35, is local to the devices and web servers it is protecting." Throughout the rejection, the Examiner utilizes Sultan's network address translation gateway 20 to render obvious Applicants' claims (see Sultan's Figure 1, below). Sultan expressly teaches that the firewall 35 is too expensive and powerful to be employed efficiently at remote LAN sites needing to establish a VPN with the main computing site (col. 7, lines 58-63). Sultan expressly teaches that the firewall 35 will have the capability to run encryption and other security applications (col. 7, lines 53-55), implying that such a firewall does not require the protection of NAT. As the Examiner has relied upon the network address translation gateway 20 to attempt to render obvious Applicants' claims, Sultan does not teach the network address translation gateway 20 connected between a Web server 40 and a computer network 50.



Sultan, Fig. 1

As a result, at least because the combination of Birkle and Sultan do not render obvious steps C, D, E, and F of claim 28 and furthermore because both Birkle and Sultan teach away from the Examiner's suggested combination, the Examiner has failed to provide a prima facie case of obviousness with respect to claim 28.

Claim 29

Regarding claim 29, it appears that the Examiner alleges that Birkle teaches step R, forwarding a response via the associated said local router to the requesting remote browser. Applicants respectfully disagree because, as stated previously, Birkle does not teach the router of steps C, D, E, and F and therefore does not teach forwarding anything externally via that router.

The Examiner alleges that the Birkle reference fails to teach ignoring requests. Applicants respectfully disagree. Per the discussion above, Birkle fails to disclose the limitations of step C, connecting a local router between said Web server and a computer network, and, as a result, further fails to disclose the limitations of steps D, E, F, and R.

The Examiner alleges that Sultan teaches the remaining method steps of claim 29. Applicants respectfully disagree. Sultan does not teach step M, determining in response to a requesting remote Web browser the destination network address it is requesting, at col. 2, line 65 through col. 3, line 11. Col. 2, line 65 through col. 3, line 11 simply details the NAT confirmation process between two remote machines. In other words, the gateway receives a reply from the internet *after* it has sent a message. At that cite, the gateway is not responding to a request from a remote Web browser, but is instead confirming a prior packet it has sent on behalf of a local machine.

For Applicants' step N, Sultan does not teach ignoring the request in response to the destination network address being for a remote web server at col. 4, lines 50-54. Instead, per the following citation, Sultan only teaches discarding a message if the source and destination ports are not Port 500: "[t]hat is, ISAKMP messages from either computer must identify Port 500 as both the source and destination port addresses. If either computer receives a packet in which Port 500 is not specified as being both the source and destination, the packet will be discarded." Additionally, read in the context of the entire paragraph, the rejection only takes place if two computers are attempting to establish a secure communication pursuant to the Internet Security Association and Key Management Protocol (ISAKMP). Therefore, Sultan does not address ignoring a request when the destination network address is for a remote web server.

Sultan does not teach Applicants' step P, operating the associated local web server to check the source network address of the web browser making the request at col. 5, lines 60-67. Instead, Sultan details how the gateway ignores other UDP datagrams from the external network having Port 500 source and destination addresses that do not match the bound Port 500 source and destination addresses.

A valid reply will be a datagram having a source IP address 1: that is the same as the external IP address that is associated with Port 500, and will have both the source and destination port addresses as Port 500. While awaiting a valid reply, the gateway will ignore other datagrams from the external network having Port 500 source and destination port addresses, but not the proper source IP address.

Sultan does not teach step Q, responding to the request via the associated said local web server using remote privileges if the source network address is that of a remote browser at col. 3, lines 42-45: "[t]he AH (Authentication Header) protocol assures data integrity, source authentication, and incorporates 'anti-repeat' measures to deter denial-of-service attacks." Applicants respectfully request the Examiner to detail how the citation applies to a gateway/router responding to a request via an associated web server using remote privileges when a datagram has a network address of a remote browser.

As a result, at least because the combination of Birkle and Sultan do not teach steps C, D, E, F, M, N, P, Q, and R of claim 29, the Examiner has failed to provide a prima facie case of obviousness.

Claim 31

The Examiner alleges that the Birkle reference fails to teach ignoring requests. Applicants respectfully disagree. Per the discussion above, Birkle fails to disclose the limitations of step C, connecting a local router between said Web server and a computer network, and, as a result, fails to disclose the limitations of steps D, E, F.

The Examiner alleges that the Sultan reference teaches Applicants' step T, responding to the request via the associated said local web server using local privileges if the source network address is that of a requesting local Web browser at col. 3, lines 42-45: "[t]he AH (Authentication Header) protocol assures data integrity, source authentication, and incorporates 'anti-repeat' measures to deter denial-of-

service attacks." Applicants respectfully request the Examiner to detail how the citation applies to a gateway/router responding to a request via an associated web server using local privileges when a datagram has a network address of a local browser.

As a result, at least because the combination of Birkle and Sultan do not teach steps C, D, E, F, and T of claim 31, the Examiner has failed to provide a prima facie case of obviousness.

In sum, because the combination of Birkle and Sultan fails to teach all of the limitations of claims 28, 29, and 31 and because both Birkle and Sultan teach away from Applicants' claimed method, the Examiner has failed to establish a prima facie case of obviousness with respect to claims 28, 29, and 31. Accordingly, Applicants respectfully request that claims 28, 29, and 31 be passed to allowance.

Additionally, claims 29 and 31 are dependent upon claim 28, which has been shown allowable above. Therefore, since claims 29 and 31 introduce additional subject matter that, when considered in the context of the recitations of claim 28, constitute patentable subject matter, Applicants submit that the recitations of claims 29 and 31 are not rendered obvious by the combination of Birkle and Sultan and respectfully request that claims 29 and 31 be passed to allowance.

Second Claim Rejection Under 35 U.S.C. § 103:

Claims 30 and 32 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Birkle in view of Sultan, in further view of Crater, et al. (USPN 5,805,442) (Crater).

Claims 30 and 32 are dependent upon claims 29 and 31, which both depend from claim 28, all of which have been shown allowable above. Therefore, since claims 30 and 32 introduce additional subject matter that, when considered in the context of the recitations of claims 28, 29, and 31 constitute patentable subject matter, Applicants submit that the recitations of claims 30 and 32 are not rendered obvious by the combination of Birkle, Sultan, and Crater and respectfully request that claims 30 and 32 be passed to allowance.

CONCLUSION

Accordingly, it is believed that the present application now stands in condition for allowance. Early notice to this effect is earnestly solicited. Should the examiner believe a telephone call would expedite the prosecution of the application, he/she is invited to call the undersigned attorney at the number listed below.

It is not believed that any fee is due at this time. If that belief is incorrect, please debit deposit account number 01-1375. Also, the Commissioner is authorized to credit any overpayment to deposit account number 01-1375.

Respectfully submitted,

Date: **February 12, 2009**

/Patricia E. McQueeney/
Patricia E. McQueeney
Registration No. 49,083

Air Liquide
2700 Post Oak Blvd., 18th Floor
Houston, Texas 77056
Phone: 302-286-5458
Fax: 713-624-8950